

**Notice of Allowability**

Application No.

09/782,825

Examiner

Longbit Chai

Applicant(s)

DISANTO ET AL.

Art Unit

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 1/20/2006.
2. ☒ The allowed claim(s) is/are 1,2,5-10 and 29.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 3/3/2006
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

CHRISTOPHER REVAK  
PRIMARY EXAMINER

*CEL* 3/7/06

### **DETAILED ACTION**

Claims 1, 2, 5 – 10 and 29 are pending for examination.

#### ***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Edward J. Howard (Reg. No. 42,670) on 3/3/2006.

This application has been amended as follows:

#### **IN THE CLAIMS**

Replace claim 1 as follows.

Claim 1:     A computer implemented method for facilitating secure electronic communications among at least two parties over a communication network, comprising:

- retaining a first private key and transmitting a corresponding first initial public key and synchronizing indicator;
- using a received second public key and second synchronizing indicator in combination with said retained first private key to determine, and retain, a first encryption key;

determining a second private key, a third public key and a third synchronizing indicator, wherein said second private key is retained with said first retained private key;

encrypting at least said third synchronizing indicator using said first encryption key;

transmitting said third public key and encrypted third synchronizing indicator;

decrypting a received fourth synchronizing indicator using said first encryption key; and

determining a second encryption key from retained said second private key, a received fourth public key and [[said]] decrypted said received fourth synchronizing indicator; [[,]]

wherein said second encryption key is retained with said first encryption key, and

said first and second encryption keys are dependent upon said second and fourth synchronizing indicators, respectively, such that if said first and second encryption keys are determined using different synchronizing indicators, data encrypted using said first and second encryption keys provides different encrypted data, respectively, and wherein said synchronizing indicators are used to alter the starting position of the encrypting sequence with the corresponding public keys.

***Allowable Subject Matter***

1. Claims 1, 2, 5 – 10 and 29 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 1 and subsequent dependent claims.

The prior arts Gennaro, alone or in combination with Bjerrum, fail to teach or suggest a method for facilitating secure electronic communications among at least two parties over a communication network, comprising: retaining a first private key and transmitting a corresponding first initial public key and synchronizing indicator; using a received second public key and second synchronizing indicator in combination with said retained first private key to determine, and retain, a first encryption key, wherein said synchronizing indicators are used to alter the starting position of the encrypting sequence with the corresponding public keys; determining a second private key, a third public key and a third synchronizing indicator, wherein said second private key is retained with said first retained private key; encrypting at least said third synchronizing indicator using said first encryption key; transmitting said third public key and encrypted third synchronizing indicator; decrypting a received fourth synchronizing indicator using said first encryption key; and determining a second encryption key from retained said second private key, a received fourth public key and [[said]]J decrypted said received

Art Unit: 2131

fourth synchronizing indicator; ([,]) wherein said second encryption key is retained with said first encryption key, and said first and second encryption keys are dependent upon said second and fourth synchronizing indicators, respectively, such that if said first and second encryption keys are determined using different synchronizing indicators, data encrypted using said first and second encryption keys provides different encrypted data, respectively.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
LBC

Longbit Chai  
Examiner  
Art Unit 2131

CHRISTOPHER REVAK  
PRIMARY EXAMINER

  
3/6/06